UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X
UNITED STATES OF AMERICA,

-against-

ALONZO SHIPP,

Defendant.
----------X

MEMORANDUM & ORDER

19-CR-029 (NGG)

NICHOLAS G. GARAUFIS, United States District Judge.

Defendant Alonzo Shipp ("Shipp" or "Defendant") moves to suppress evidence obtained from his Facebook account. (See Mots. to Suppress (Dkt. 20); Mem. in Support of Mots. to Suppress ("Mem.") (Dkt. 20-1).)[1] For the following reasons, the court DENIES Defendant's motion.

I. BACKGROUND

A. Facts[2]

1. Alleged Shooting

On or about July 20, 2018, an unnamed individual, referred to herein as John Doe, was shot in the vicinity of 117-26 147th Street in Queens, New York. (Compl. (Dkt. 1) ¶ 2.) Doe then ran south down 147th Street and east on 119th Street to the corner of 119th Avenue and Sutphin Boulevard, where he collapsed. (Id.)

---

[1] Shipp also moved to suppress post-arrest statements and identification evidence, or in the alternative for an evidentiary hearing as to whether law enforcement engaged in a deliberate two-step interrogation of Shipp, and a Wade hearing. (See Mem. at 5.) Only the motion to suppress the Facebook warrant (the "Facebook Motion") is before the court at this time. (See May 23, 2019 Order (granting Government's request to address only the Facebook Motion at this time in light of the Government's representation that it would not seek to introduce post-arrest statements or an identification of Shipp if the court denied his motion to suppress the Facebook warrant).)

[2] The court assumes the parties' familiarity with the factual background and sets forth here only those facts relevant to the Facebook Motion.

Video of the incident shows an individual wearing a white t-shirt pointing an object at another individual. (Id. ¶ 3.) A muzzle flash is visible. (Id.) The video then shows Doe running south on 147th Street. (Id.)

Doe then called 911 and stated in part: "I've been shot . . . My shooter's coming to me right now . . . My shooter is on me . . . My shooter is right here, my shooter is right here" and "I don't want to die Pump, please. Please [inaudible] Pump. Pump. Pump. I don't want to die Pump. Pump I don't want to die, Pump." (Id. ¶¶ 4, 6.)

Video cameras captured footage of Doe on Sutphin Boulevard. (Id. ¶ 7.) The footage shows an individual approach Doe, take an item out of his pants or waistband, stand over Doe, point an object at him, and then walk away. (Id.) As he walked away, his face was visible on a surveillance camera. (Id.) Surveillance video of the incident also appears to show the alleged shooter wearing a bandage or similar object on his lower left arm. (Aff. in Supp. of an Appl. for a Search Warrant ("Aff.") (Dkt. 25-1) ¶ 7.)

On January 2, 2019, Shipp was arrested and charged with possession of the firearm alleged to have been used in the July 20, 2018 incident. (See Mem. at 6; Indictment (Dkt. 7) ¶ 1.)

2. Facebook Warrant

On February 8, 2019, Magistrate Judge Vera M. Scanlon signed a search and seizure warrant authorizing disclosure of information associated with Facebook user ID 100002075016114 (the "Facebook Warrant"). (See Facebook Warrant (Dkt. 25-1) at ECF p. 17-22.) The warrant application was based on the affidavit of Special Agent Joanna Beck of the Bureau of Alcohol, Tobacco, Firearms, and Explosives (the "Affidavit"). (See Aff. at ECF p. 2-16.) The Affidavit set forth the basis for probable cause, which included the following:

- During a 911 call placed during the alleged shooting, the victim can be heard calling the shooter "Pump." (Id.)
- Surveillance video of the incident on July 20, 2018 appear to show the shooter wearing a bandage or similar object on his lower left arm. (Id. ¶ 7.)
- Shipp has admitted that he uses the nickname "Pump." (Id.)
- Publicly accessible photos, including a profile picture, on a Facebook account belonging to a user calling himself "Sts Pistol Tony" appear to be photos of Shipp, indicating that the account may belong to Shipp. (Id. ¶ 9.)
- Individuals wish the account holder "Happy Birthday" on October 31, the date of Shipp's birthday. (Id.)
- Publicly available photos from May 25, 2018 from this account show Shipp with what appears to be an ACE bandage on his lower left arm fewer than two months before the date of the shooting. (Id. ¶ 10.)[3]
- Publicly available posts from 2018 on the account appear to show Shipp referring to himself as "Pump" and other individuals referring to him as "Pump." (Id. ¶ 11.)

The Facebook Warrant required Facebook to disclose to the Government a substantial amount of information pertaining to the user ID identified:

(a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook

[3] This fact is relevant because, as noted above, the alleged shooter in the surveillance video of the incident appeared to be wearing bandage or similar object on his lower left arm at the time of the alleged shooting. (See Aff. ¶ 7.)

security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

(b) All activity logs for the account and all other documents showing the user's posts and other Facebook activities;

(c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them;

(d) All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

(e) All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests;

(f) All "check ins" and other location information;

(g) All IP logs, including all records of the IP addresses that logged into the account;

(h) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";

(i) All information about the Facebook pages that the account is or was a "fan" of;

(j) All past and present lists of friends created by the account;

(k) All records of Facebook searches performed by the account;

(l) All information about the user's access and use of Facebook Marketplace;

(m) The types of service utilized by the user;

(n) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

(o) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

(p) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

(Facebook Warrant, Attach. B-I.)

The Facebook Warrant also authorized law enforcement officers to seize "[a]ll information described above in Section I that constitutes evidence of a violation of 18 U.S.C. § 922(g) involving Alonzo Shipp since January 1, 2018, including . . . information pertaining to the following matters:"

(a) Evidence of the possession of firearms by Shipp;

(b) Evidence indicating how Shipp went by the nickname "Pump" and/or that other individuals knew him by the name "Pump";

(c) Evidence demonstrating that Shipp had a bandage on his left arm in or about the time of the shooting;

(d) Evidence indicating how and when the Facebook account was accessed or used to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Facebook account owner (including,

but not limited to, whether Shipp was in or around Queens, New York at the time of the shooting in July 2018);

(e) Evidence indicating the Facebook account owner's state of mind as it relates to the crime under investigation;

(f) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(Id. Attach. B-II.)

Pursuant to the Facebook Warrant, Facebook disclosed 21,471 pages. (Opp'n to Facebook Mot. ("Opp'n") (Dkt. 25) at 4.) On April 25, 2019, the Government produced to Shipp the entire return from Facebook. (Id.) The Government states that law enforcement agents are continuing to review this return to determine which parts may be seized pursuant to Attachment B-II. (Id.) To date, the Government has seized several pieces of evidence pursuant to Attachment B-II, including:

- Evidence demonstrating that the account belongs to Shipp.
- A status update posted by the account user six days before the shooting, in which he referred to himself as "Pump," and a message in November 2018 in which the account user told another individual to call him and stated: "my name is pump";
- Messages sent by the account user six days after the shooting, in which he stated that he needed money and was on the run. When asked why he was on the run, the account user responded, "I know u seen the news a shooting." When the individual said she had not seen the news and asked where the shooting has happened, the account user stated, "119 sutphin." When the other individual

asked if anyone was hurt, the account user wrote, "of course they got my pics." He later added that he had already left town.

- Messages sent by Defendant in November 2018, in which he forwarded a post by the NYPD from September 10, 2018 that included a photograph of Shipp and an appeal for the public to help locate him "in regards to a nonfatal shooting." The person to whom the account user sent the post responded, "O, my goshhh. sigh." and the account user responded, "I know." Later in the conversation, when the individual told the account user that this information hurts them, the account user wrote, "Im hurt to cuz I was chilling into this incident."

(Id. at 4-6.)

B. Procedural History

On January 2, 2019, Shipp was arrested and charged with possession of the firearm alleged to have been used in the July 20, 2018 incident. (See Mem. at 6; Indictment (Dkt. 7) ¶ 1.) He was denied bail on January 10, 2019. (See Jan. 10, 2019 Min. Entry (Dkt. 4); Order of Detention (Dkt. 5).) Shipp was arraigned on February 1, 2019 before Magistrate Judge Scanlon, at which point he entered a plea of not guilty. (Feb. 1, 2019 Min. Entry (Dkt. 11).)

Shipp now seeks to suppress evidence uncovered from the Facebook account because, he contends, the warrant was overbroad and not sufficiently particular. (See Mots.; Mem.) The Government opposes the motion, arguing that the Facebook Warrant met the particularity requirement and was not overbroad, and that in any case, the good-faith exception would apply. (Id. at 12-13.)

II. LEGAL STANDARD

The Fourth Amendment explicitly commands that warrants must be based on probable cause and must "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. The warrant requirement is intended to ensure that "those searches deemed necessary should be as limited as possible." Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971). "It is familiar history that indiscriminate searches and seizures conducted under the authority of 'general warrants' were the immediate evils that motivated the framing and adoption of the Fourth Amendment." United States v. Ulbricht, 858 F.3d 71, 99 (2d Cir. 2017), cert. denied, 138 S. Ct. 2708 (2018) (quoting Payton v. New York, 445 U.S. 573, 583 (1980)). "Those general warrants 'specified only an offense,' leaving 'to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched.'" Id. (quoting Steagald v. United States, 451 U.S. 204, 220 (1981)). The principal defect in such a warrant was that it permitted a "general, exploratory rummaging in a person's belongings," Andresen v. Maryland, 427 U.S. 463, 480 (1976) (citation and internal quotation marks omitted), a problem that the Fourth Amendment attempted to resolve by requiring the warrant to "set out with particularity" the "scope of the authorized search," Kentucky v. King, 563 U.S. 452, 459 (2011).

The appropriate scope of a search "is defined by the object of the search and the places in which there is probable cause to believe that it may be found." United States v. Ross, 456 U.S. 798, 824 (1982). Therefore, "[j]ust as probable cause to believe that a stolen lawnmower may be found in a garage will not support a warrant to search an upstairs bedroom, probable cause to believe that undocumented aliens are being transported in a van will not justify a warrantless

search of a suitcase." Id. Similarly, "[p]robable cause to believe that a container placed in the trunk of a taxi contains contraband or evidence does not justify a search of the entire cab." Id.

To be sufficiently particular under the Fourth Amendment, a warrant must satisfy three requirements. Ulbricht, 858 F.3d at 99. First, "a warrant must identify the specific offense for which the police have established probable cause." United States v. Galpin, 720 F.3d 436, 445 (2d Cir. 2013) (citations omitted). Second, "a warrant must describe the place to be searched." Id. at 445-46 (citations omitted). Finally, the "warrant must specify the items to be seized by their relation to designated crimes." Id. at 446 (internal quotation marks omitted).

Despite their frequent conflation, "[over]breadth and particularity are related but distinct concepts. A warrant may be broad, in that it authorizes the government to search an identified location or object for a wide range of potentially relevant material, without violating the particularity requirement." Ulbricht, 858 F.3d at 102. Similarly, "[w]hen the criminal activity pervades [an] entire business, seizure of all records of the business is appropriate, and broad language used in warrants will not offend the particularity requirements." Id. (quoting U.S. Postal Serv. v. C.E.C. Servs., 869 F.2d 184, 187 (2d Cir. 1989)). In determining whether a warrant is overbroad, courts must focus on "whether there exists probable cause to support the breadth of the search that was authorized." United States v. Zemlyansky, 945 F. Supp. 2d 438, 464 (S.D.N.Y. 2013)

"Even if a warrant lacks particularity, '[t]he fact that a Fourth Amendment violation occurred . . . does not necessarily mean that the exclusionary rule applies.'" United States v. Lin, No. 15-CR-601 (DLI), 2018 WL 3416524, at *6 (E.D.N.Y. July 11, 2018) (quoting Herring v. United States, 555 U.S. 135, 140 (2009)). The Supreme Court has held that "exclusion 'has always been our last resort, not our first impulse,' and our precedents establish important

principles that constrain application of the exclusionary rule." Herring, 555 U.S. at 140 (internal citation omitted). "Although in a particular case it may not be easy to determine when an affidavit demonstrates the existence of probable cause, the resolution of doubtful or marginal cases in this area should be largely determined by the preference to be accorded to warrants." United States v. D'Amico, 734 F. Supp. 2d 321, 359 (S.D.N.Y. 2010) (quoting United States v. Smith, 9 F.3d 1007, 1012 (2d Cir. 1993)).

III. DISCUSSION

A. Overbreadth and Particularity

The court has serious concerns regarding the breadth of Facebook warrants like the one at issue here.[4] The Second Circuit has observed that "[a] general search of electronic data is an especially potent threat to privacy because hard drives and e-mail accounts may be 'akin to a residence in terms of the scope and quantity of private information [they] may contain.'" Ulbricht, 858 F.3d at 99 (quoting Galpin, 720 F.3d at 445); see also Galpin, 720 F.3d at 447 (explaining that "[t]his threat demands a heightened sensitivity to the particularity requirement in the context of digital searches"). This threat is further elevated in a search of Facebook data because, perhaps more than any other location—including a residence, a computer hard drive, or a car—Facebook provides a single window through which almost every detail of a person's life is visible.[5] Indeed, Facebook is designed to replicate, record, and facilitate personal, familial,

[4] Courts have recognized a Fourth Amendment interest in the data contained in an individual's Facebook account. See United States v. Meregildo, 883 F. Supp. 2d 523, 525 (S.D.N.Y. 2012) (noting that "[w]hen a social media user disseminates his postings and information to the public, they are not protected by the Fourth Amendment," but that "postings using more secure privacy settings reflect the user's intent to preserve information as private and may be constitutionally protected" (citing Katz, 389 U.S. at 351-52 (1967)).

[5] Modern cell phones may provide the closest analogy to a Facebook account because, as the Supreme Court explained in Riley v. California, 573 U.S. 373 (2014), mobile phone applications "offer a range of tools for managing detailed information about all aspects of a person's life" such that "many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—

social, professional, and financial activity and networks. Users not only voluntarily entrust information concerning just about every aspect of their lives to the service, but Facebook also proactively collects and aggregates information about its users and non-users in ways that we are only just beginning to understand. See, e.g., Josh Constine, Facebook's new Study app pays adults for data after teen scandal, TECHCRUNCH, June 11, 2019, https://techcrunch.com/2019/06/11/study-from-facebook/ (describing various apps Facebook has built and launched that, once installed, send all the data on a person's phone to Facebook); Sarah Frier and Todd Shields, Zuckerberg Says Facebook Collects Internet Data on Non-Users, BLOOMBERG, Apr. 11, 2018, https://www.bloomberg.com/news/articles/2018-04-11/zuckerberg-says-facebook-collects-internet-data-on-non-users (describing Facebook's practice of tracking nonusers' internet activity); Natasha Singer, What You Don't Know About How Facebook Uses Your Data, N.Y. TIMES, Apr. 11, 2018, https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html (explaining that Facebook tracks users and non-users, collects biometric facial data, and "can learn almost anything about you by using artificial intelligence to analyze your behavior"). (See also Aff. ¶ 27 (explaining that "Facebook also provides its users with access to thousands of other applications ('apps') on the Facebook platform")). Particularly troubling, information stored in non-Facebook applications may come to constitute part of a user's "Facebook account"—and thus be subject to broad searches—by virtue of corporate decisions, such as mergers and integrations, without the act or awareness of any particular user. See Alex Hern, EU data watchdog raises concerns over Facebook integration, THE GUARDIAN, Jan. 28, 2019, https://www.theguardian.com/technology/2019/jan/28/eu-data-watchdog-raises-concerns-

---

from the mundane to the intimate." Id. at 395 (explaining that "[t]he average smart phone user has installed 33 apps, which together can form a revealing montage of the user's life).

facebook-integration (discussing privacy concerns arising from Facebook's plans to merge three messaging networks that it owns—Facebook Messenger, WhatsApp, and Instagram). It is thus hard to imagine many searches more invasive than a search of all the data associated with a Facebook account. Cf. Riley, 573 U.S. at 394 ("The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions.").

The Second Circuit has cautioned that "[b]ecause of the nature of digital storage, it is not always feasible to 'extract and segregate responsive data from non-responsive data.'" Ulbricht, 858 F.3d 99-100 (quoting Galpin, 720 F.3d at 447 (internal quotation marks omitted)). As the Government notes, courts in this circuit have applied this rationale to Facebook data in upholding warrants similar to the one at issue here. (Opp'n at 9-10.) See, e.g., United States v. Westley, No. 17-CR-171 (MPS), 2018 WL 3448161, at *12 (D. Conn. July 17, 2018) (in upholding Facebook warrant, equating Facebook information to other "electronic evidence" and asserting that "extremely broad" disclosure is a "practical necessity when dealing with electronic evidence"); United States v. Liburd, No. 17-CR-296 (PKC), 2018 WL 2709199, at *3 (E.D.N.Y. June 5, 2018) (upholding broad Facebook search warrant "because of the nature of digital searches"); United States v. Tairod Nathan Webster Pugh, No. 15-CR-00116 (NGG), 2015 WL 9450598, at *5 (E.D.N.Y. Dec. 21, 2015) (upholding Facebook warrant where the affidavit indicated that the defendant used his Facebook account as a means and method of committing the charged crime—attempting to join a terrorist group, and analogizing Facebook searches and other digital searches). However, Facebook is different from hard drives or email accounts in many ways, including that the information associated with the account is categorized and sorted by the company—not by the user. For this reason, Facebook is less like other areas of the "digital realm, where the size or other outwardly visible characteristics of a file may disclose

nothing about its content," see Galpin, 720 F.3d at 447, and more akin to a physical location, in which "the physical dimensions of the evidence sought will naturally impose limitations on where an officer may pry: an officer could not properly look for a stolen flat-screen television by rummaging through the suspect's medicine cabinet, nor search for false tax documents by viewing the suspect's home video collection," see id. The concerns present in the search of a hard drive or email account—that evidence sought could be located almost anywhere—and which necessitate broad digital search protocols do not, therefore, exist in the Facebook context. For example, there is no possibility that a user could have filed an incriminating photo as a "poke," and there is no chance that an incriminating message will be stored as a third-party password or a rejected friend request. As the Eleventh Circuit has observed:

> The means of hiding evidence on a hard drive—obscure folders, misnamed files, encrypted data—are not currently possible in the context of a Facebook account. Hard drive searches require time-consuming electronic forensic investigation with special equipment, and conducting that kind of search in the defendant's home would be impractical, if not impossible. By contrast, when it comes to Facebook account searches, the government need only send a request with the specific data sought and Facebook will respond with precisely that data. That procedure does not appear to be impractical for Facebook or for the government. Facebook produced data in response to over 9500 search warrants in the six-month period between July and December 2015.

United States v. Blake, 868 F.3d 960, 974 (11th Cir. 2017), cert. denied sub nom. Moore v. United States, 138 S. Ct. 753 (2018), and cert. denied, 138 S. Ct. 1580 (2018) (citations omitted). Compared to other digital searches, therefore, Facebook searches both (1) present a greater "risk that every warrant for electronic information will become, in effect, a general warrant," Ulbricht, 858 F.3d at 99, and (2) are more easily limited to avoid such constitutional concerns. In light of these considerations, courts can and should take particular care to ensure that the scope of searches involving Facebook are "defined by the object of the search and the places in which

there is probable cause to believe that it may be found." See United States v. Ross, 456 U.S. 798, 824 (1982); see also Blake, 868 F.3d at 974 (citations omitted) (where Facebook warrant "required disclosure to the government of virtually every kind of data that could be found in a social media account," observing that if the request before them had been more limited in time and limited to the crime at issue, it "would have undermined any claim that the Facebook warrants were the internet-era version of a 'general warrant'"). In so doing, courts should be sensitive to the substantive differences between different types of digital data. See Riley, 573 U.S. at 395 (observing that "certain types of [digital] data are also qualitatively different").

Like many Facebook search warrants, the warrant at issue here authorized a very broad search, but permitted the actual "seizure" only of certain information constituting evidence of the crime of being a felon in possession after January 1, 2018. (See Facebook Warrant.) The Facebook Warrant required the disclosure to the government of sixteen categories of information associated with the Facebook account, a seemingly boilerplate list apparently designed to capture all information associated with the account. Accordingly, Facebook provided 21,000 pages of information to the government, which included all contact and personal identifying information, all private messages and chat histories, all video history, all activity logs (including logs of activity in associated Facebook applications), all friend requests, all rejected friend requests, all photoprints, all Neoprints, and all past and present lists of friends. The Facebook Warrant even required the disclosure of information generated in connection with services that appear entirely unrelated to the facts in the Affidavit and the crime charged—for example, there was no fact in the Affidavit suggesting that the account holder used Facebook Marketplace, a service that can be used to buy and sell items and services online, let alone that Facebook Marketplace would

contain evidence of the charged crime of being a felon in possession or even additional evidence that the account belonged to Shipp.

Moreover, although the Facebook Warrant only permitted the government to seize "evidence of a violation of 18 U.S.C. § 922(g) involving ALONZO SHIPP since January 1, 2018," the government was permitted to search the entire Facebook account since its creation. (Facebook Warrant, Attach. B-II.) "A warrant's failure to include a time limitation, where such limiting information is available and the warrant is otherwise wide-ranging, may render it insufficiently particular." Zemlyansky, 945 F. Supp. 2d at 464 (citation, quotation marks, and alterations omitted) (finding that the absence of a temporal limit on items to be searched "reinforces the Court's conclusion that the [] warrant functioned as a general warrant"). Although a temporal limitation for the data being searched is not "an absolute necessity," see United States v. Hernandez, No. 09-CR-625 (HB), 2010 WL 26544, at *11 (S.D.N.Y. Jan. 6, 2010) (noting that a "temporal limitation" is an "indic[ium] of particularity"), it would appear to have been feasible to include such a limitation here.[6] Doing so could have mitigated the court's concerns about the breadth of this warrant. See Blake, 868 F.3d at 974 (observing that Facebook warrants "should have requested data only from the period of time during which [the defendant] was suspected of taking part in the [charged crime]"). For example, the Affidavit did not articulate probable cause to believe that a search of Shipp's rejected friend requests from years earlier would reveal evidence showing that Shipp possessed a firearm in 2018.

Finally, the court notes that the warrant did not set any limits on what the Government was required to do with the information that they collected and searched, but did not "seize."

[6] Given that Facebook controls the storage and cataloging of associated data, and that digital data is generally sortable by date stamps, temporal limitation of Facebook searches appears feasible.

This is concerning in light of the breadth of information that Facebook was required to provide to the Government pursuant to the Facebook Warrant. See In Matter of Search of Info. Associated with Facebook Account Identified by Username Aaron.Alexis that is Stored at Premises Controlled by Facebook, Inc., 21 F. Supp. 3d 1, 11 (D.D.C. 2013) (noting that although Federal Rule of Criminal Procedure 41 creates a distinction between material to be "disclosed" and material to be "seized," "even the material that is not within this second 'seizure' category will still be turned over to the government, and it will quite clearly be 'seized' within the meaning of that term under the Fourth Amendment"). But cf. Galpin, 720 F.3d at 451 (noting that the Second Circuit has "not required specific search protocols or minimization undertakings as basic predicates for upholding digital search warrants," and declining to "impose any rigid requirements in that regard at this juncture").

In sum, the court is concerned that Facebook warrants of the kind at issue here unnecessarily "authorize precisely the type of 'exploratory rummaging' the Fourth Amendment protects against." See United States v. Bradbury, No. 14-CR-71, 2015 WL 3737595, at *4 (N.D. Ind. June 15, 2015) (finding that warrant that did not limit the scope of a search of defendant's Facebook account appeared on its face to permit an "inappropriate" "exploratory search"). Indeed, the format of the Facebook Warrant—an enumerated list of sixteen different categories of information associated with the account—suggests the organized nature of data associated with a Facebook account. It thus provides support for Defendant's contention that the search authorized by the Facebook Warrant could have been more clearly defined by its object—i.e., evidence of possession of a firearm in 2018—and limited to the categories of information associated with the Facebook account in which there was probable cause to believe that such evidence might be found. (See Reply at 5.) Cf. Galpin, 720 F.3d at 451-52 (explaining that the

plain view exception is not available to the extent that "digital search protocols target information outside the scope of the valid portion of the warrant," noting that there was little evidence in the record as to whether the search at issue was "directed—much less properly limited—to those files that would substantiate [the charged crime]," and ordering the district court on remand to "determine whether a search limited to evidence of a registration violation would have necessitated the opening of image files or the playing of video files").

B. Good Faith Exception

That said, the court need not decide whether the Facebook Warrant violated the Fourth Amendment because, even if it did, the Facebook Warrant falls into the "good faith exception" to the exclusionary rule established by United States v. Leon, 468 U.S. 897 (1984). See Blake, 868 F.3d at 974 (declining to decide whether broad Facebook warrants violated the Fourth Amendment because the court founds that the good-faith exception applied). As the Second Circuit has noted, "suppression is 'our last resort, not our first impulse' in dealing with violations of the Fourth Amendment." United States v. Clark, 638 F.3d 89, 99 (2d Cir. 2011) (quoting Herring v. United States, 555 U.S. 135 (2009) (quotation marks and citations omitted)). The extent to which exclusion is justified "varies with the culpability of the law enforcement conduct." Id. (quoting Herring, 555 U.S. at 143). Thus, evidence should not be excluded where it was "obtained in objectively reasonable reliance on a subsequently invalidated search warrant." Id. (quoting Leon, 468 U.S. at 922). When an officer genuinely believes that he has obtained a valid warrant from a magistrate and executes that warrant in good faith, there is no conscious violation of the Fourth Amendment, "and thus nothing to deter." United States v. Raymonda, 780 F.3d 105, 118 (2d Cir. 2015) (quoting Leon, 468 U.S. at 920-21).

"The burden is on the government to demonstrate the objective reasonableness of the officers' good faith reliance on an invalidated warrant." Clark, 638 F.3d at 100 (citation and quotation marks omitted). In assessing whether it has carried that burden, the Second Circuit has cautioned that "in Leon, the Supreme Court strongly signaled that most searches conducted pursuant to a warrant would likely fall within [the] protection [of the good-faith exception]." Id. "[A]gainst this presumption of reasonableness," the Supreme Court has identified four circumstances where an exception to the exclusionary rule would not apply:

> (1) where the issuing magistrate has been knowingly misled; (2) where the issuing magistrate wholly abandoned his or her judicial role; (3) where the application is so lacking in indicia of probable cause as to render reliance upon it unreasonable; and (4) where the warrant is so facially deficient that reliance upon it is unreasonable.

Id. (quoting United States v. Moore, 968 F.2d 216, 222 (2d Cir. 1992)); see Leon, 468 U.S. at 923.

Neither the first nor the second parameter have any applicability here. With respect to the other two parameters, the court finds that the Facebook Warrant was not "based on an affidavit so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable," Leon, 468 U.S. at 923 (citation and quotation marks omitted), nor was it "so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers c[ould not have] reasonably presume[d] it to be valid," id. (citation omitted). The Affidavit articulated probable cause to search at least certain categories of information or services associated with the Facebook account, and as the Government notes, other district courts have declined to suppress evidence obtained pursuant to facially similar warrants. See, e.g., Liburd, 2018 WL 2709199, at *3; Westley, 2018 WL 3448161, at *12; Pugh, 2015 WL 9450598. Therefore, although the court has serious concerns about the breadth of the search authorized here and in similar cases, it nonetheless finds that reliance on the Facebook

Warrant by law enforcement officers was not objectively unreasonable. Application of the exclusionary rule in this case would thus serve little deterrent purpose.

IV. CONCLUSION

For the foregoing reasons, Defendant's (Dkt. 20) motion to suppress evidence obtained pursuant to the Facebook Warrant is DENIED.

SO ORDERED.

s/Nicholas G. Garaufis

Dated: Brooklyn, New York
July 11, 2019

NICHOLAS G. GARAUFIS
United States District Judge